The following claims are presented for examination:

The following claims are presented for examination:

1. (Currently Amended) A method comprising:

detecting, at a server, that a device is attempting to connect to a network;

receiving, at the server, a token from the device, wherein the token is in one of:

- **i. a first state in which the content of the token indicates that the token has not been modified by the device, and**
- **ii. a second state in which the content of the token indicates that the token has been modified by the device, wherein when the token is in the second state, the content of the token comprises:**
  - **– an indication that the execution of a security software application executing on the device was suspended, and**
  - **– an identification of a network to which the device was connected when the execution of the security software application was suspended;**

when the token is in the second state, determining**, at the server,** if **[[a]]** **the** device was previously connected to an untrusted network; and

if the device was connected to an untrusted network, evaluating the integrity of ~~**some of the**~~ data on the device**, wherein the integrity evaluation is performed by at least one of the device and the server** ~~**when the device was previously connected to the untrusted network**~~.

2. (Canceled)

3. (Currently Amended) The method of claim 1, wherein **the scope of the integrity evaluation depends on the frequency at which the device connects to the network identified by the token when the token is in the second state** ~~**determining further comprises determining if the device connected to at least one unknown network**~~.

4. (Currently Amended) The method of claim 1, **comprising** ~~**wherein**~~:

permitting, at the server, the device to connect to a the network on a first port, when the token is in the first state; and

permitting, at the server, the device to connect the network on a second port when the token is in the second state; and

wherein only frames that are necessary for content restoration are permitted to flow between the network and the device when the device is connected to the network on the second port.

~~**evaluating further comprises determining if a token on the device has been altered.**~~

5. (Previously Presented) The method of claim 1, wherein determining further comprises logging an address of each network that the device connected to.

6. (Canceled)

7. (Currently Amended) The method of claim 1, wherein the scope of the evaluation is based on ~~**one or more defined**~~ **a** content authentication **rule** ~~**rules**~~.

8. (Previously Presented) The method of claim 1, wherein evaluating further comprises performing a virus scan.

9. (Currently Amended) An apparatus comprising:
a memory; and

a processor, coupled to the memory, for:

detecting that a device is attempting to connect to a network;

receiving a token from the device, wherein the token is in one of:

i. a first state in which the content of the token indicates that the token has not been modified by the device, and

ii. a second state in which the content of the token indicates that the token has been modified by the device, wherein when the token is in the second state, the content of the token comprises:

– an indication that the execution of a security software executing on the device was suspended, and

– an identification of a network to which the device was connected when the security software was suspended;

when the received token is in the second state, determining if **[[a]]** **the** device was previously connected to an untrusted network; and

if the device was connected to an untrusted network, evaluating the integrity of ~~**some of the**~~ data on the device ~~**when the device was previously connected to the untrusted network**~~.

10. (Currently Amended) The apparatus of claim 9, wherein **the scope of the integrity check depends on the frequency at which the device connects to the network identified by the token when the token is in the second state** ~~**determining further comprises determining if the device connected to at least one unknown network**~~.

11. (Original) The apparatus of claim 9, wherein the processor is further configured to evaluate a log of addresses of each network that the device accessed.

12. (canceled)

13. (Original) The apparatus of claim 9, wherein the scope of the evaluation is based on one or more defined content authentication rules.

14-23 (Canceled).